AUTORITE DE REGULATION DES TELECOMMUNICATIONS/TIC DE CÔTE D'IVOIRE

POLE RESSOURCES ET TECHNOLOGIES

CENTRE SPECIALISE CI-CERT

RAPPORT ANNUEL 2018

SOMMAIRE

AVANT-PROPOS

Le présent document est le rapport annuel d'activités du Centre de veille et de réponse aux incidents de sécurité inforamtique dénommé Côte d'Ivoire Computer Emergency response Team (CI-CERT). Comme les précédentes années, il relate les principales activités et les résultats obtenus au cours de l'année 2018 en matière de protection du cyberespace ivoirien et de la lutte contre la cybercriminalité.

Ce rapport rend compte des activités menées par le CI-CERT pour accompagner l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI) dans sa mission de sécurisation et de protection des réseaux et assurer une confiance dans l'utilisation des Technologies de l'Information et de la Communication.

I. PRESENTATION DU CI-CERT

Le CERT National dénommé Côte d'Ivoire Computer Emergency Response Team (CI-CERT) a été créé en Juin 2009.

Les missions du CI-CERT sont :

- Assurer la coordination du traitement des incidents de sécurité informatique au niveau national pour les acteurs des secteurs privé et public ;
- Contribuer à la lutte contre la cybercriminalité ;
- Contribuer à assurer la sécurité des infrastructures critiques de l'Etat ;
- Assurer la veille technologique en matière de sécurité de l'information ;
- Sensibiliser la population sur les dangers liés à l'utilisation des TIC.

I. BILAN DES ACTIVITES REALISEES EN 2018

1. Au titre de la cybersécurité et de la lutte contre la cybercriminalité

a. Traitement d'incidents de sécurité informatique

Le traitement des incidents est un service réactif qui consiste à recevoir, trier et répondre aux demandes et aux signalements, et à analyser les incidents et évènements. Les actions de réponse peuvent plus particulièrement consister à :

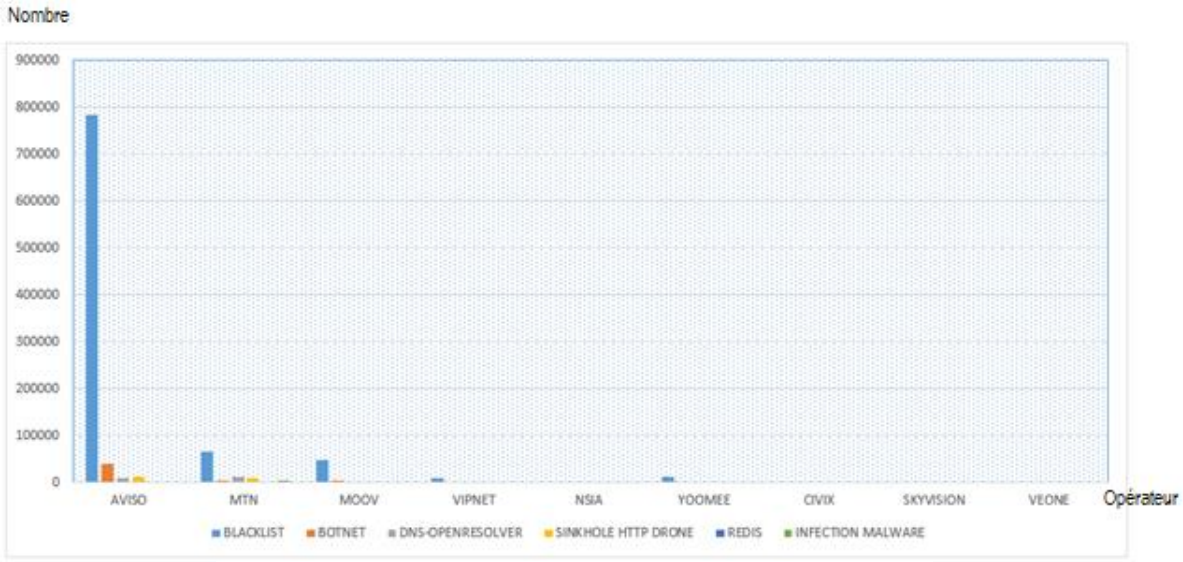
- Prendre des mesures pour protéger les systèmes et réseaux concernés ou menacés par une intrusion ;

- Proposer des solutions et des actions d'atténuation à partir des alertes et bulletins de sécurité pertinents ;
- Rechercher une activité éventuelle de l'intrus sur d'autres parties du réseau ;
- Filtrer le trafic sur le réseau ;
- Restaurer les systèmes ;
- Appliquer des correctifs aux systèmes ou les réparer ;
- Développer d'autres stratégies de réponse ou solutions temporaires.

Ainsi le CI-CERT a traité au cours de cette année 2018, **1 026 790 incidents** soit **une baisse de 3,7%** comparé à l'année 2017. Ces incidents sont constitués majoritairement à 86,72% d'adresses IP « blacklistées » et 5,21% liés au Botnet[1].

Cette baisse s'explique en partie par les formations offertes depuis deux (02) ans par le CI-CERT aux parties prenantes sur le traitement avancé des incidents de sécurité informatique et à la présence d'équipe de sécurité informatique au sein des opérateurs et FAI.

Les détails des activités sont consignés dans le graphique ci-après :



Graphique 1 : Type d'incidents par opérateurs et FAI

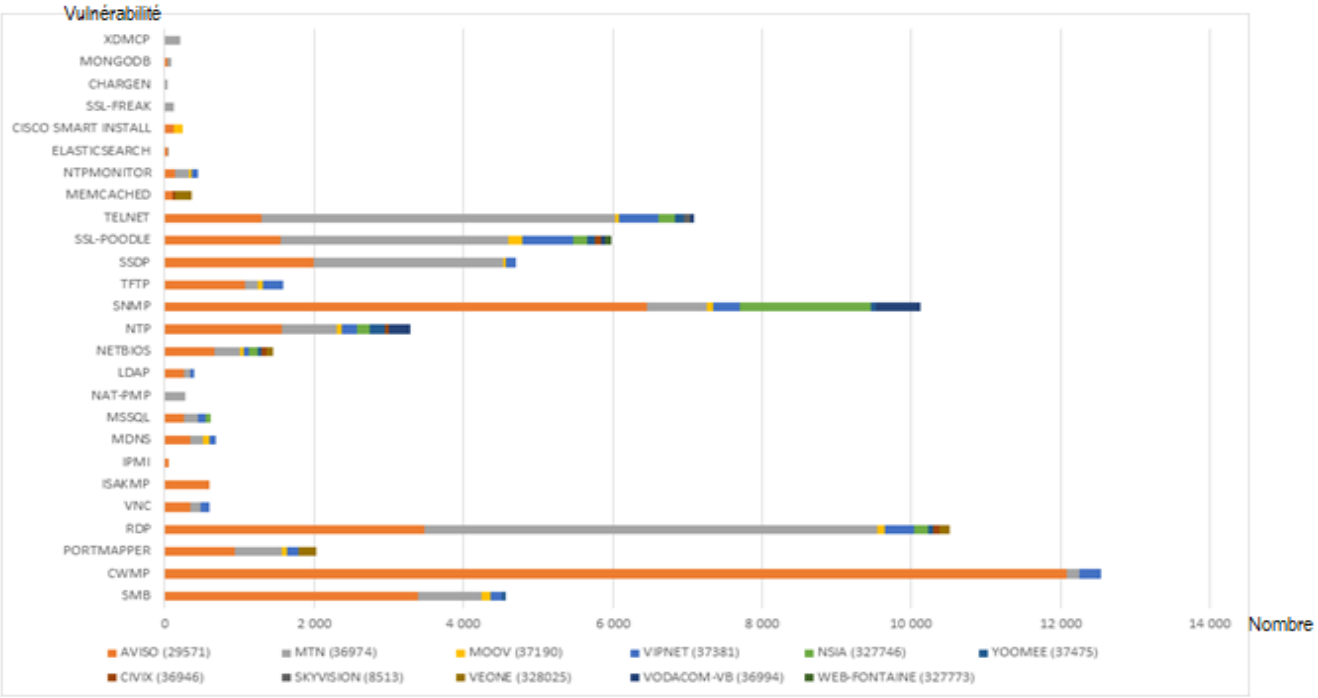
Les adresses IP gérées par le Fournisseur d'Accès à Internet AVISO de l'opérateur Orange CI ont connu le nombre d'incidents le plus élevé avec 848 147 incidents soit 82,60%, suivi des opérateurs MTN avec 96 309 soit 9,38% et MOOV avec 55053 soit 5,36%.

b. Coordination des vulnérabilités

[1] Un **botnet** est un réseau d'ordinateurs infectés par un logiciel malveillant afin qu'ils puissent être contrôlés à distance, les forçant ainsi à envoyer des pourriels, à répandre des virus ou à réaliser des attaques DDoS à l'insu des véritables propriétaires des ordinateurs et sans leur approbation

Le CI-CERT avertit les différentes parties prenantes de l'existence de vulnérabilités, correctifs ou solutions temporaires y afférents et fournit des informations sur les moyens d'y remédier ou d'en atténuer les effets.

Pour cette année, **68 655 vulnérabilités** ont été notifiées aux parties prenantes impactées contre 48.350 en 2017 soit une hausse d'environ **42%** par rapport à 2017.



Graphique 2 : Nombre de vulnérabilités par mois et par opérateurs

Les adresses IP des Fournisseurs d'Accès à Internet AVISO (Orange CI) et MTN CI ont été les plus exposées avec respectivement 36 810 (**53,61%)** et 21 623 (**31,50%**) vulnérabilités détectées.

Ces vulnérabilités sont la conséquence des faiblesses dans la conception, la mise en œuvre ou l'utilisation des composants matériel ou logiciels des systèmes d'information et surtout le non–respect des bonnes pratiques de sécurité et des mesures d'hygiène informatique.

c. Veille technologique et Sensibilisation

- **Publications d'informations de sécurité : alertes, bulletins et avis de sécurité**

Le CI-CERT a publié sur son site Internet au cours de l'année 2018, trois cent deux **(302**) bulletins de sécurité dont quatorze (**14**) *alertes de sécurité* via ses différents canaux de distribution (Site Web et Mailing-List), contre deux cent quatre-vingt-trois (283) en 2017 soit une augmentation de **6,7%.**

- **Sensibilisation**

En sensibilisant d'avantage l'ensemble des parties prenantes sur la problématique de la cybersécurité, le CI-CERT permet non seulement de mieux comprendre les questions de sécurité, mais également d'exécuter leurs tâches courantes de manière plus sûre. Cette activité contribue à réduire le nombre des attaques et à augmenter la probabilité de voir les parties prenantes détecter et signaler les attaques dont elles sont victimes, ce qui réduirait les délais de reprise et supprimerait, ou du moins minimiserait, les pertes.

Le CI-CERT publie via son site web et les réseaux sociaux des articles, des bulletins d'information, des guides et d'autres ressources d'information pour expliquer les bonnes pratiques et recommander certaines précautions en matière de sécurité informatique sur des thématiques portant sur le :

- Ransomware ;
- Phishing ;
- Mot de passe fort (Double authentification) ;
- Escroquerie en ligne ;
- Etc.

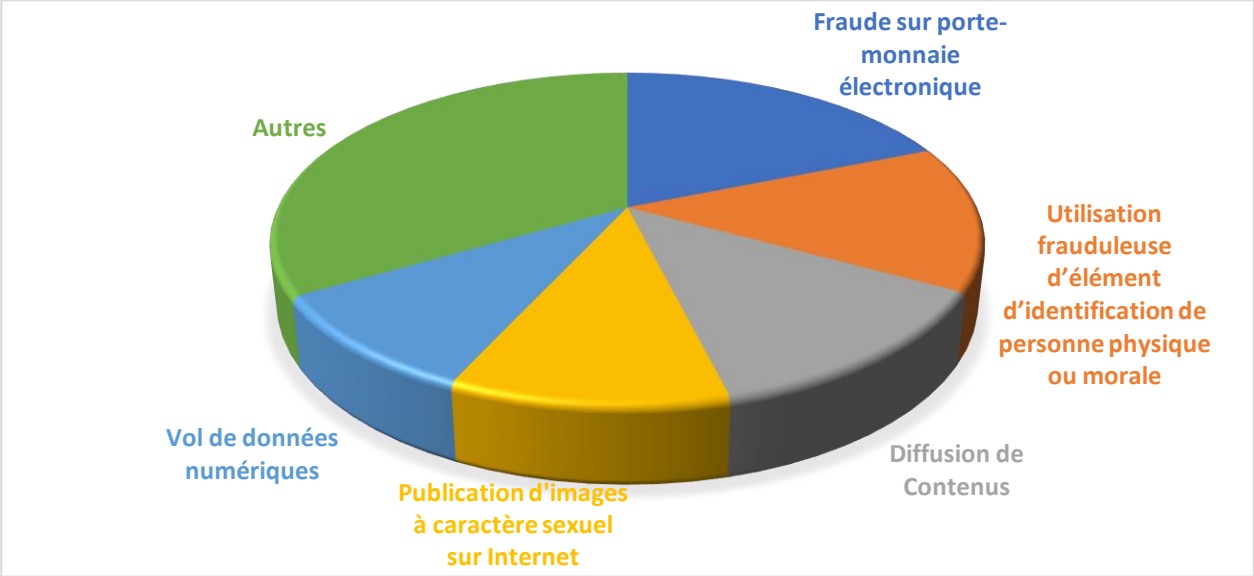
d. Lutte contre la cybercriminalité

Au titre de la lutte contre la Cybercriminalité, cette activité est menée par la Plateforme de Lutte Contre la Cybercriminalité (PLCC) qui est le fruit de l'accord de partenariat signé en 2011 et actualisé le 27 janvier 2014, entre la Direction Générale de la Police Nationale (DGPN) et l'ARTCI. Cet accord de partenariat a été à nouveau actualisé le **10 juillet 2017**.

Le préjudice financier des dossiers de cybercriminalité est estimé à **7 414 071 997 FCFA** en 2018 contre **5 172 126 471 FCFA** en 2017, soit une augmentation de 43%.

Comparé à 2017, le nombre d'affaires/plaintes a légèrement augmenté, passant de **2.408** à **2.860** en 2018, soit une augmentation d'environ **19 %.**

Cette année 2018, 93% des plaintes proviennent de la Côte d'Ivoire suivie de la France (1%), et quatre-vingt-neuf (89) personnes ont été interpellées pour soixante-treize (73) cybercriminels déférés.



Graphique 3 : Préjudices financiers par type d'infraction

Les infractions en 2018 sont constituées essentiellement de :

- Fraude sur porte-monnaie électronique (18,81%) ;
- Utilisation frauduleuse d'élément d'identification de personnes physiques ou morales (14,23%) ;
- Diffusions de contenus illicites (13,08%) ;
- Publications d'images à caractère sexuel (10,73%).

e. Autres activités

- **Renforcement des capacités en faveur des équipes informatiques de l'administration publique**

Le CI-CERT a animé une formation à l'endroit des DSI de l'administration publique du 14 au 25 mai 2018 à la salle de conférences du 17ème étage de la tour C. cette session a vu la participation d'une quarantaine de responsables IT, issus de différents ministères. Cette session avait pour but d'une part de présenter le CI-CERT et ses missions et d'autre part de former les auditeurs sur les questions de cybersécurité notamment sur la gestion des risques, la politique générale de sécurité et la gestion des incidents de sécurité.

- **Renforcement de capacité de l'équipe du CI-CERT par le CERT/CC**

Une mission de formation conduite par le CERT/CC des Etats-Unis a eu lieu du 22 au 26 janvier 2018 à l'ARTCI. Cette formation a porté sur le thème « DDoS and Network Analysis ». Cette formation a vu la participation de nos parties prenantes habituelles notamment les FAI et les Opérateurs et avait pour objectifs de :

- Identifier les informations pertinentes nécessaires à l'analyse des réseaux ;
- Traiter les incidents informatiques de type DDoS ;
- Détecter les vulnérabilités exploitées et à l'origine des attaques DDoS ;
- Diffuser et publier les informations de sécurité selon des procédures bien définies.

Parallèlement à cette formation destinée aux techniciens, des discussions entre les managers venus des Etats-Unis et ceux de l'ARTCI ont porté sur l'état d'avancement des actions menées l'accompagnement du CERT/CC, les actions à venir et la stratégie pour la montée en puissance du CI-CERT.

- **Cyber Drill national**

Le jeudi 20 septembre 2018 s'est tenue une formation en ligne portant sur le contenu scientifique du CyberDrill national prévu dans le plan d'action de la collaboration avec le CERT/CC. Cette formation s'est faite à distance via l'outil Skype Entreprise, entre les experts américains du CERT/CC et les membres de l'équipe du CI-CERT accompagnée des agents des centres spécialisés. L'objectif était de former l'équipe du CI-CERT sur le contenu, la méthodologie et l'organisation technique de cet exercice qui sera faite à l'intention des gestionnaires des systèmes d'information de l'administration publique.

III. PERSPECTIVES 2019

Pour l'année 2019, le CI-CERT s'est fixé de nombreux défis à relever pour contribuer au développement d'une économie numérique dans un environnement favorable, inspirant la confiance des utilisateurs des technologies de l'information et de la communication. Ce sont :

- L'organisation d'un séminaire de formation en cybersécurité pour les gestionnaires des systèmes d'information de l'administration ;
- La poursuite de la collaboration avec le CERT/CC et le département d'ETAT des Etats-Unis pour le renforcement des capacités opérationnelles du CI-CERT ;
- La formalisation de la collaboration avec les acteurs de la sécurité de l'écosystème numérique en Côte d'Ivoire ;
- Etc.

Lexique

- **Blacklist** : Répertoires d'adresses IP qui ont été identifiées par les différents FAIs et webmails comme générant beaucoup de spam. En d'autres termes, si une adresse IP est inscrite sur la liste noire d'un service d'emailing, cela signifie que son utilisateur a de fortes chances d'être un spammeur.

- **CcTLD** : Un domaine de premier niveau national (en anglais country code top-level domain ou **ccTLD**) est un type de domaines de premier niveau (TLD) maintenus par l'Internet Assigned Numbers Authority (IANA) pour une utilisation dans le système de nom de domaine d'Internet.

- **Whois :** Service de recherche fourni par les registres Internet, par exemple les Registres Internet régionaux ou bien les registres de noms de domaine permettant d'obtenir des informations sur une adresse IP ou un nom de domaine.

- **Phishing :** L'hameçonnage, phishing ou filoutage est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité.

- **DNS-Openresolver :** DNS fournissant la résolution récursive de nom pour les clients à l'extérieur de son domaine administratif.

- **Sinkhole Drone** : Machine cible utilisée par les chercheurs pour recueillir des informations sur un botnet particulier.

- **Attack Malicious :** Attaque malicieuse.

- **Spam :** Le « spam » ou « pollupostage », désigne les communications électroniques massives, notamment de courrier électronique, non sollicitées par les destinataires, à des fins publicitaires ou malhonnêtes : le pourriel contient généralement de la publicité.

- **Scan : (Port Scan)** En informatique, le balayage de ports (port scanning en anglais) est une technique servant à rechercher les ports ouverts sur un serveur de réseau. ... Les balayages de ports se font habituellement sur le protocole TCP ; néanmoins, certains logiciels permettent aussi d'effectuer des balayages UDP.

- **Virus :** Programme écrit dans le but de se propager sournoisement et rapidement à d'autres ordinateurs. Il perturbe plus ou moins gravement le fonctionnement de l'ordinateur infecté.

- **Redis :** (de l'anglais REmote DIctionary Server qui peut être traduit par « serveur de dictionnaire distant » et jeu de mot avec Redistribute1) est un système de gestion de base de données clef-valeur scalable, très hautes performances, écrit en C ANSI et distribué sous licence BSD.

- Le **Domain Name System** (ou **DNS**, système de noms de domaine) est un service permettant de traduire un nom de domaine en informations de plusieurs types qui y sont associées, notamment en adresses IP de la machine portant ce nom.

- **Mailing-List :** Liste des récipiendaires des informations de sécurité informatique.

- **Fraude sur le porte-monnaie électronique :** Un appel ou un SMS est émis à l'endroit de la victime lui demandant de saisir des codes (USSD) pour bénéficier d'un prétendu bonus ou pour valider la réception de son transfert. A l'insu de la victime, sa carte SIM est désactivée et réactivée sur une nouvelle puce. Le détenteur de la nouvelle puce a alors un contrôle total de ses comptes électroniques.

- **Code USSD :** Message constitué de suite de caractères, envoyés comme commande au réseau de téléphonie afin d'y exécuter des programmes.

- **Utilisation frauduleuse d'éléments d'identification de personnes physiques et/ou morale :** Cette infraction consiste pour le cybercriminel à usurper l'identité d'une personne physique ou morale pour se faire passer pour celle-ci afin de soit demander de l'aide financière à ses correspondants, soit pour proposer des produits ou des services.

- **Atteinte à l'image (à la cyber réputation) :** Le droit pénal offre plusieurs textes permettant de protéger son e-réputation lorsqu'elle est atteinte aux moyens des réseaux sociaux notamment.

- **Injure :** Toute expression outrageante, termes de mépris ou invective qui ne renferme l'imputation d'aucun fait. (Ex : le PDG de l'entreprise X est un voleur etc.)

- **Diffamation :** Allégation ou imputation d'un fait qui porte atteinte à l'honneur ou à la considération de la personne.

- **La divulgation de la vie privée :** elle concerne spécifiquement la vie sentimentale d'une personne, la publication d'informations concernant la santé d'une personne, puis le droit à l'image.

- **Vol de données informatiques** : Le cyber délinquant s'approprie frauduleusement les informations numériques de sa victime à des fins délictueuses.